UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/766,174	01/28/2004	Timothy S. Olson	CISCO-6592	4436

21921   7590   01/04/2007
DOV ROSENFELD
5507 COLLEGE AVE
SUITE 2
OAKLAND, CA 94618

EXAMINER
BRANDT, CHRISTOPHER M

ART UNIT	PAPER NUMBER
2617	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Office Action Summary	10/766,174	OLSON ET AL.
	Examiner	Art Unit	
	Christopher M. Brandt	2617	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>29 January 2004</u>.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-29</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-29</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>29 January 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>See Continuation Sheet</u>.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :2/24/04, 12/9/04, 8/8/05, 8/22/05, 2/14/06, 3/17/06, & 4/28/06.

DETAILED ACTION

Priority

Receipt is acknowledged of papers submitted claiming the benefit of U.S. Provisional

Application No. 60/490,847, filed on July 28, 2003, which papers have been placed of record in

the file.

Information Disclosure Statement

The information disclosure statements submitted on 02/24/2004, 12/09/2004, 08/08/2005,

08/22/2005, 02/14/2006, 03/17/2006, and 04/28/2006 have been considered by the Examiner and

made of record in the application file.

Claim Objections

The claims are objected to because the lines are crowded too closely together, making

reading difficult. Substitute claims with lines one and one-half or double spaced on good quality

paper are required. See 37 CFR 1.52(b).

Claim 18 objected to because of the following informalities: On line 21 of claim 18 there

is a period after 'AP' with further limitations following the period. It is noted that only one

period may be used per claim. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
subject matter which the applicant regards as his invention.

Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing

to particularly point out and distinctly claim the subject matter which applicant regards as the

invention.

Consider **claim 2**. The word "substantially" on **line 2 of claim 2** is considered as being indefinite for failing to particularly point out and distinctly claim the subject matter. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 26-27 are rejected under 35 USC 101 because the claimed invention is directed to non-statutory subject matter. The language of the claim raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory matter under 35 USC 101.

Claims 26-27 claims the non-statutory subject matter of a program. Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1754 (claim to a data structure per se held nonstatutory). Therefore, since the claimed programs (i.e., carrier medium) are not tangibly embodied in a physical medium and encoded on a computer-readable medium, the Applicants have not complied with 35 USC 101.

The Examiner suggests changing **claims 26-27** from "a carrier medium carrying one or more computer-readable code segments" to -- computer-readable medium encoded with computer readable instructions --. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the

claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various

claims was commonly owned at the time any inventions covered therein were made absent any

evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out

the inventor and invention dates of each claim that was not commonly owned at the time a later

invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c)

and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness
       or nonobviousness.

Claims 1-29 are rejected under 35 USC 103(a) as being unpatentable over **FUJII et al.**

(US PGPUB 2003/0117985 A1) in view of **Whelan et al. (US PGPUB 2004/0003285 A1)**.

Consider **claim 1**. FUJII et al. (hereinafter Fujii) disclose a method comprising:

maintaining an AP database that includes information about managed access point (APs) and friendly APs of a wireless network (paragraphs 33, 38, read as the calculating section 21 comprises an AP list comparing section 26 having a function of comparing an AP list obtained with a registered AP list. In addition, these AP lists (i.e. databases) include information on clients that can be deleted and/or added (i.e. maintained)), including the data of each managed AP (paragraph 38, read as an SSID as an ID number identifying equipment with which the client is to communicate are added to the AP list in the AP list storage section 19);

sending a scan request to one or more managed APs of the wireless network , the scan request including one or more of a request for the receiving managed AP to scan for beacons and probe responses and a request for the receiving managed AP to request the AP's clients to scan for beacons and probe responses (paragraph 38, read as figure 5 is a flow chart showing a flow of a process executed for a scan and AP search operation by the AP search section 16 of the transmitting and receiving section 15. The client determines whether or not a beacon has been able to be received via the antenna 18. if the client determines that a beacon has been received, an SSID as an ID number identifying equipment with which the client is to communicate are added to the AP list in the AP list storage section 19);

receiving reports from at least one of the receiving managed APs (paragraph 42, read as the AP list receiving section 28 of the transmitting and receiving section 25 receives AP lists transmitted by the clients 10a to 10e), a report including information on any beacon or probe response received that was sent by an AP (paragraph 42, read as the management AP list contains genuine access points permitted to access the network), including the data of the beacon/probe response sending AP (paragraphs 39 and 43, read as if the client determines that a

beacon has been received, an SSID as an ID number identifying equipment with which the client

is to communicate are added to the AP list in the AP list storage section 19); and

for each beacon or probe response on which information is received; analyzing the

information received in the report about the AP that sent the beacon or probe response, the

analyzing including ascertaining if the data of the AP that sent the beacon or probe response

matches a data of an AP in the AP database to ascertain whether or not the AP is an illegal AP or

a managed or friendly AP (paragraphs 44 and 45, read as the collected AP list is compared with ·

the registered AP list to extract those APs in the collected AP lists which are not registered in the

registered AP list, i.e. illegal APs).

Fujii discloses the claimed invention except he fails to explicitly state rogue AP and

MAC address.

However, Whelan et al. (hereinafter Whelan) disclose rogue AP and MAC address

(paragraph 39, read as the network monitor may also attempt to disable communications between

the network and the rogue access point form the network. In one embodiment, the monitor

changes the MAC address filter settings on the rogue access point to exclude all MAC

addresses).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to have incorporated the teachings of Whelan into the method of Fujii in

order to identify and prevent the use of the network by the rogue access point (paragraph 39).

Consider **claim 18**. Fujii discloses a method comprising:

receiving a scan request at an AP of a wireless network to scan for beacons and probe responses, the request received from a WLAN manager (paragraph 19, read as a wireless LAN device that can be connected to a computer (i.e. the controller 20 is read as the WLAN manager)) managing a set of managed APs and client stations of the managed APs, the managing including maintaining an AP database that contains information about managed APs and friendly APs of the wireless network, the information in the AP database including the data of each managed AP (paragraphs 38 and 40, read as figure 5 is a flow chart showing a flow of a process executed for a scan and AP search operation by the AP search section 16 of the transmitting and receiving section 15. The client determines whether or not a beacon has been able to be received via the antenna 18. If the client determines that a beacon has been received, an SSID as an ID number identifying equipment with which the client is to communicate are added to the AP list in the AP list storage section 19. The AP list dispatching section 17 (client) of the transmitting section 15 dispatches the AP list thus obtained to the controller 20);

one or both of listening for beacons and probe responses at the AP receiving the scan request or sending a client request to one or more client stations associated with the AP receiving the scan request to listen for beacons and probe responses (paragraphs 38, read as figure 5 is a flow chart showing a flow of a process executed for a scan and AP search operation by the AP search section 16 of the transmitting and receiving section 15);

in the case that a client request was sent, receiving a client report at the AP from at least one of the wireless stations to which the client request was sent, the client report including information on any beacon or probe response received from an illegal AP (paragraph 42, read as the management AP list contains genuine access points permitted to access the network),

including the data of the beacon/probe response sending AP (paragraphs 39 and 43, read as if the

client determines that a beacon has been received, an SSID as an ID number identifying

equipment with which the client is to communicate are added to the AP list in the AP list storage

section 19); and

sending a scan report to the WLAN manager including information on any beacon or

probe response received from an illegal AP by the AP receiving the scan request or in the case

that a client request was sent, by any client stations from a report was received, the information

including the data of the illegal AP (paragraph 38, read as figure 5 is a flow chart showing a flow

of a process executed for a scan and AP search operation by the AP search section 16 of the

transmitting and receiving section 15. The client determines whether or not a beacon has been

able to be received via the antenna 18. if the client determines that a beacon has been received,

an SSID as an ID number identifying equipment with which the client is to communicate are

added to the AP list in the AP list storage section 19).

such that for each beacon or probe response on which information is received at the

WLAN manager, analyzing the information received in the report about the illegal AP that sent

the beacon or probe response, including ascertaining if the data of the illegal AP matches a data

of an AP in the AP database leads to ascertaining whether or not the potential AP is likely to be

an illegal AP (paragraph 44, read as data on APs actually connected to the network is obtained,

as a collected AP list, from the AP lists collected from the clients. Then, the collected AP list is

compared with the registered AP list to extract those APs in the collected AP lists which are not

registered in the registered AP list, i.e. illegal APs).

Fujii discloses the claimed invention except he fails to explicitly state rogue AP and MAC address.

However, Whelan et al. (hereinafter Whelan) disclose rogue AP and MAC address (paragraph 39, read as the network monitor may also attempt to disable communications between the network and the rogue access point form the network. In one embodiment, the monitor changes the MAC address filter settings on the rogue access point to exclude all MAC addresses).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated the teachings of Whelan into the method of Fujii in order to identify and prevent the use of the network by the rogue access point (paragraph 39).

Consider **claim 26**. Fujii discloses a carrier medium carrying one or more computer-readable code segments to instruct one or more processors of a processing system to execute a method comprising (paragraph 19, read as storage medium storing a program):

maintaining an AP database that includes information about managed access point (APs) and friendly APs of a wireless network (paragraphs 33, 38, read as the calculating section 21 comprises an AP list comparing section 26 having a function of comparing an AP list obtained with a registered AP list. In addition, these AP lists (i.e. databases) include information on clients that can be deleted and/or added (i.e. maintained)), including the data of each managed AP (paragraph 38, read as an SSID as an ID number identifying equipment with which the client is to communicate are added to the AP list in the AP list storage section 19);

sending a scan request to one or more managed APs of the wireless network , the scan

request including one or more of a request for the receiving managed AP to scan for beacons and

probe responses and a request for the receiving managed AP to request the AP's clients to scan

for beacons and probe responses (paragraph 38, read as figure 5 is a flow chart showing a flow of

a process executed for a scan and AP search operation by the AP search section 16 of the

transmitting and receiving section 15. The client determines whether or not a beacon has been

able to be received via the antenna 18. if the client determines that a beacon has been received,

an SSID as an ID number identifying equipment with which the client is to communicate are

added to the AP list in the AP list storage section 19);

receiving reports from at least one of the receiving managed APs (paragraph 42, read as

the AP list receiving section 28 of the transmitting and receiving section 25 receives AP lists

transmitted by the clients 10a to 10e), a report including information on any beacon or probe

response received that was sent by an AP (paragraph 42, read as the management AP list

contains genuine access points permitted to access the network), including the data of the

beacon/probe response sending AP (paragraphs 39 and 43, read as if the client determines that a

beacon has been received, an SSID as an ID number identifying equipment with which the client

is to communicate are added to the AP list in the AP list storage section 19); and

for each beacon or probe response on which information is received; analyzing the

information received in the report about the AP that sent the beacon or probe response, the

analyzing including ascertaining if the data of the AP that sent the beacon or probe response

matches a data of an AP in the AP database to ascertain whether or not the AP is a potential

rogue AP or a managed or friendly AP (paragraphs 44 and 45, read as the collected AP list is

compared with the registered AP list to extract those APs in the collected AP lists which are not

registered in the registered AP list, i.e. illegal APs).

Fujii discloses the claimed invention except he fails to explicitly state rogue AP and

MAC address.

However, Whelan et al. (hereinafter Whelan) disclose rogue AP and MAC address

(paragraph 39, read as the network monitor may also attempt to disable communications between

the network and the rogue access point form the network. In one embodiment, the monitor

changes the MAC address filter settings on the rogue access point to exclude all MAC address).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to have incorporated the teachings of Whelan into the method of Fujii in

order to identify and prevent the use of the network by the rogue access point (paragraph 39).

Consider **claim 27**. Fujii discloses a carrier medium carrying one or more computer-

readable code segments to instruct one or more processors of a processing system to execute a

method at an AP of a wireless network comprising (paragraph 19, read as storage medium

storing a program):

receiving a scan request at an AP of a wireless network to scan for beacons and probe

responses, the request received from a WLAN manager (paragraph 19, read as a wireless LAN

device that can be connected to a computer (i.e. the controller 20 is read as the WLAN manager))

managing a set of managed APs and client stations of the managed APs, the managing including

maintaining an AP database that contains information about managed APs and friendly APs of

the wireless network, the information in the AP database including the data of each managed AP

(paragraphs 38 and 40, read as figure 5 is a flow chart showing a flow of a process executed for a

scan and AP search operation by the AP search section 16 of the transmitting and receiving

section 15. The client determines whether or not a beacon has been able to be received via the

antenna 18. If the client determines that a beacon has been received, an SSID as an ID number

identifying equipment with which the client is to communicate are added to the AP list in the AP

list storage section 19. The AP list dispatching section 17 (client) of the transmitting section 15

dispatches the AP list thus obtained to the controller 20);

one or both of listening for beacons and probe responses at the AP receiving the scan

request or sending a client request to one or more client stations associated with the AP receiving

the scan request to listen for beacons and probe responses (paragraphs 38, read as figure 5 is a

flow chart showing a flow of a process executed for a scan and AP search operation by the AP

search section 16 of the transmitting and receiving section 15);

in the case that a client request was sent, receiving a client report at the AP from at least

one of the wireless stations to which the client request was sent, the client report including

information on any beacon or probe response received from an illegal AP (paragraph 42, read as

the management AP list contains genuine access points permitted to access the network),

including the data of the beacon/probe response sending AP (paragraphs 39 and 43, read as if the

client determines that a beacon has been received, an SSID as an ID number identifying

equipment with which the client is to communicate are added to the AP list in the AP list storage

section 19); and

sending a scan report to the WLAN manager including information on any beacon or

probe response received from an illegal AP by the AP receiving the scan request or in the case

that a client request was sent, by any client stations from a report was received, the information

including the data of the illegal AP (paragraph 38, read as figure 5 is a flow chart showing a flow

of a process executed for a scan and AP search operation by the AP search section 16 of the

transmitting and receiving section 15. The client determines whether or not a beacon has been

able to be received via the antenna 18. if the client determines that a beacon has been received,

an SSID as an ID number identifying equipment with which the client is to communicate are

added to the AP list in the AP list storage section 19).

such that for each beacon or probe response on which information is received at the

WLAN manager, analyzing the information received in the report about the illegal AP that sent

the beacon or probe response, including ascertaining if the data of the illegal AP matches a data

of an AP in the AP database leads to ascertaining whether or not the potential AP is likely to be

an illegal AP (paragraph 44, read as data on APs actually connected to the network is obtained,

as a collected AP list, from the AP lists collected from the clients. Then, the collected AP list is

compared with the registered AP list to extract those APs in the collected AP lists which are not

registered in the registered AP list, i.e. illegal APs).

Fujii discloses the claimed invention except he fails to explicitly state rogue AP and

MAC address.

However, Whelan et al. (hereinafter Whelan) disclose rogue AP and MAC address

(paragraph 39, read as the network monitor may also attempt to disable communications between

the network and the rogue access point form the network. In one embodiment, the monitor

changes the MAC address filter settings on the rogue access point to exclude all MAC

addresses).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to have incorporated the teachings of Whelan into the method of Fujii in

order to identify and prevent the use of the network by the rogue access point (paragraph 39).

Consider **claim 28**. Fujii discloses an apparatus comprising:

a processing system including a memory and a network interface to couple the apparatus

to a network, the network including a set of managed access points (APs) of a wireless network,

and

an AP database coupled to the processing system and containing information about the

managed access point and friendly APs of the wireless network (paragraphs 33, 38, read as the

calculating section 21 comprises an AP list comparing section 26 having a function of comparing

an AP list obtained with a registered AP list. In addition, these AP lists (i.e. databases) include

information on clients that can be deleted and/or added (i.e. maintained)), including the data of

each managed AP (paragraph 38, read as an SSID as an ID number identifying equipment with

which the client is to communicate are added to the AP list in the AP list storage section 19),

the processing system programmed to:

send a scan request to one or more managed APs of the wireless network, the scan

request including one or more of a request for the receiving managed AP to scan for beacons and

probe responses and a request for the receiving managed AP to request the AP's clients to scan

for beacons and probe responses (paragraph 38, read as figure 5 is a flow chart showing a flow of

a process executed for a scan and AP search operation by the AP search section 16 of the transmitting and receiving section 15. The client determines whether or not a beacon has been able to be received via the antenna 18. if the client determines that a beacon has been received, an SSID as an ID number identifying equipment with which the client is to communicate are added to the AP list in the AP list storage section 19);

receive reports from at least one of the receiving managed APs, a report including information on any beacon or probe response received that was sent by an AP, including the data of any AP whose beacon/probe response was received (paragraph 42, read as the management AP list contains genuine access points permitted to access the network), including the data of the beacon/probe response sending AP (paragraphs 39 and 43, read as if the client determines that a beacon has been received, an SSID as an ID number identifying equipment with which the client is to communicate are added to the AP list in the AP list storage section 19); and

for each beacon or probe response on which information is received, analyze the information received in the report about the AP that sent the beacon or probe response, the analyzing including ascertaining if the data of the AP that sent the beacon or probe response matches data of an AP in the AP database to ascertain whether or not the AP is an illegal AP or a managed or friendly AP (paragraphs 44 and 45, read as the collected AP list is compared with the registered AP list to extract those APs in the collected AP lists which are not registered in the registered AP list, i.e. illegal APs).

Fujii discloses the claimed invention except he fails to explicitly state rogue AP and MAC address.

However, Whelan et al. (hereinafter Whelan) disclose rogue AP and MAC address

(paragraph 39, read as the network monitor may also attempt to disable communications between

the network and the rogue access point form the network. In one embodiment, the monitor

changes the MAC address filter settings on the rogue access point to exclude all MAC

addresses).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to have incorporated the teachings of Whelan into the method of Fujii in

order to identify and prevent the use of the network by the rogue access point (paragraph 39).

Consider **claim 29**. Fujii discloses an access point (AP) for a wireless network, the

access point comprising:

a processing system including a memory;

a network interface to couple the access point to a network;

a wireless transceiver coupled to the processing system to implement the PHY of a

wireless station (paragraph 33)

the processing system including a processor and programmed:

to receive a scan request to scan for beacons and probe responses, the request received

via the network interface from a WLAN manager (paragraph 19, read as a wireless LAN device

that can be connected to a computer (i.e. the controller 20 is read as the WLAN manager))

coupled to the network and managing a set of managed APs and client stations of the managed

APs, the managing including maintaining an AP database that contains information about

managed APs and friendly APs of the wireless network, including the Data of each managed AP

(paragraphs 38 and 40, read as figure 5 is a flow chart showing a flow of a process executed for a

scan and AP search operation by the AP search section 16 of the transmitting and receiving

section 15. The client determines whether or not a beacon has been able to be received via the

antenna 18. If the client determines that a beacon has been received, an SSID as an ID number

identifying equipment with which the client is to communicate are added to the AP list in the AP

list storage section 19. The AP list dispatching section 17 (client) of the transmitting section 15

.dispatches the AP list thus obtained to the controller 20);

one or both of to listen for beacons and probe responses via the PHY or to send a client

request via the PHY to one or more client stations associated with the AP to listen for beacons

and probe responses (paragraphs 38, read as figure 5 is a flow chart showing a flow of a process

executed for a scan and AP search operation by the AP search section 16 of the transmitting and

receiving section 15);

in the case that a client request was sent, to receive a client report from at least one of the

client stations to which the client request was sent, the client report including information on any

beacon or probe response received at the client station from an illegal AP (paragraph 42, read as

the management AP list contains genuine access points permitted to access the network),

including the data of the beacon/probe response sending AP (paragraphs 39 and 43, read as if the

client determines that a beacon has been received, an SSID as an ID number identifying

equipment with which the client is to communicate are added to the AP list in the AP list storage

section 19); and

to send a scan report to the WLAN manager via the network interface, including

information on any beacon or probe response received from an illegal AP by the AP receiving

the scan request or in the case that a client request was sent, by any client stations from a report

was received, the scan report including the Data of any AP whose beacon/probe response was

received (paragraph 38, read as figure 5 is a flow chart showing a flow of a process executed for

a scan and AP search operation by the AP search section 16 of the transmitting and receiving

section 15. The client determines whether or not a beacon has been able to be received via the

antenna 18. if the client determines that a beacon has been received, an SSID as an ID number

identifying equipment with which the client is to communicate are added to the AP list in the AP

list storage section 19),

such that for each beacon or probe response on which information is received at the

WLAN manager, analyzing the information received in the report about the illegal AP that sent

the beacon or probe response, including ascertaining if the Data of the illegal AP matches a Data

of an AP in the AP database leads to ascertaining whether or not the potential AP is likely to be

an illegal AP (paragraph 44, read as data on APs actually connected to the network is obtained,

as a collected AP list, from the AP lists collected from the clients. Then, the collected AP list is

compared with the registered AP list to extract those APs in the collected AP lists which are not

registered in the registered AP list, i.e. illegal APs).

Fujii discloses the claimed invention except he fails to explicitly state rogue AP and

MAC addresses.

However, Whelan et al. (hereinafter Whelan) disclose rogue AP and MAC addresses

(paragraph 39, read as the network monitor may also attempt to disable communications between

the network and the rogue access point form the network. In one embodiment, the monitor

changes the Data filter settings on the rogue access point to exclude all MAC addresses).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to have incorporated the teachings of Whelan into the method of Fujii in

order to identify and prevent the use of the network by the rogue access point (paragraph 39).

Consider **claim 2 and as applied to claim 1**. Fujii discloses a method wherein the

wireless network substantially conforms to the IEEE 802.11 standard for wireless local area

networks (paragraph 32).

Consider **claim 3 and as applied to claim 1**. Fujii discloses a method wherein the

maintaining the AP database includes updating the AP database from time to time (paragraphs 37

and 38).

Consider **claim 4 and as applied to claim 1**. Fujii discloses a method wherein the

analyzing further includes comparing information in the received report related to the beacon or

probe response with information stored in the AP database about the configuration of managed

APs (paragraph 45).

Consider **claim 5 and as applied to claim 4**. Fujii and Whelan disclose a method

wherein the analysis further includes determining the approximate location of the potential rogue

AP in order to further ascertain whether the potential rogue AP is likely to be a rogue (Fujii;

paragraphs 8 and 46; Whelan; abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated the two in order to remove / isolate the illegal / rogue access point (Fujii; paragraph 46, Whelan; abstract).

Consider **claim 6 and as applied to claim 1**. The combination of Fujii and Whelan disclose a method wherein the sending a request includes sending a request to one or more wireless stations of the wireless network to listen for beacons and probe responses on the respective serving channels of the respective stations and to report the results of the listening.

Consider **claim 7 and as applied to claim 1**. Fujii discloses a method wherein the sending a request includes sending a request for one or more wireless stations to temporarily listen for beacons and probe responses on a channel specified in the request and to report the results for listening (paragraphs 37 and 38).

Consider **claim 8 and as applied to claim 1**. Fujii and Whelan disclose a method wherein the sending a request includes sending a request for one or more managed access points to listen for beacons and probe responses and to report the results of the listening (paragraphs 38 and 40).

Consider **claim 9 and as applied to claim 1**. The combination of Fujii and Whelan disclose a method wherein the sending a request includes sending a request for one or more clients of one or more managed access points to listen for beacons and probe responses and to report the results of the listening.

Consider **claim 10 and as applied to claim 1**. Fujii discloses a method wherein the analyzing includes comparing configuration information in the beacon or probe response with information stored in the AP database about managed APs (paragraph 45).

Consider **claim 11 and as applied to claim 10**. Fujii and Whelan disclose a method wherein the analyzing further includes using timing information determined from the beacon or probe response to further ascertain whether the AP is likely to be a rogue (paragraph 42, read as it is determined whether or not the standby time has passed, which is used in order to receive AP lists).

Consider **claim 12 and as applied to claim 11**. Fujii and Whelan disclose a method wherein the analyzing further includes using known location information of managed APs together with the timing information to determine the approximate location of the potential rogue AP (paragraph 42 and 46, read as it is determined whether or not the standby time has passed, which is used in order to receive AP lists. In addition, the estimated location of the illegal AP is determined).

Consider **claims 13 and 14 and as applied to claim 10**. Fujii and Whelan disclose a method wherein the analyzing further includes using known location information of managed APs to approximately locate the potential rogue AP, and method further comprising: locating the potential rogue AP by using the RSSI at the station receiving the beacon or probe response together with a calibrated path loss model of an area of interest that provides path losses at various locations to or from managed stations at known locations and wherein the locating includes: accepting an ideal path loss model applicable to an area of interest; calibrating the ideal

path loss model using measurements received from each respective managed station of a first set

of managed wireless stations of the wireless network measuring the received signal strengths at

each of the respective managed stations, the managed stations receiving signals as a result of

transmissions by respective managed stations of a second set of managed wireless stations of the

wireless network, each respective transmission at a known respective transmit power, the

locations of each managed station of the first and second set being known or determined, the

calibrating being to determine a calibrated path loss model between the receiving and

transmitting wireless stations; receiving measurements from each respective managed station of

a third set of managed wireless stations of the wireless network measuring the received signal

strength at each of the respective stations resulting from transmission of a beacon or probe

response from a potential rogue access point, each station of the third set being at a known or

determined location; and for each of a set of assumed transmit powers for the potential rogue

access point, determining the likely location or locations of the potential rogue access point using

the received signal strengths at the stations of the third set and the calibrated path loss model

(paragraph 46 and 47, read as the warning may indicate the presence of an illegal AP and the

estimated location of the illegal AP. A diagram indicating the locations at which regularly

registered APs that can be connected to the network are installed is recorded in the HDD 23 of

the controller 20. Further, the AP lists received from the clients contain the intensities of signal

from the APS (RSSI). This allows each of the clients to determine how far it is from the location

at which each regular AP is installed and to determine the location. In the conventional wireless

LAN network, the clients perform search operations to recognize available APs, i.e. to recognize

APS that can allow electromagnetic waves to reach the clients).

Consider **claim 15 and as applied to claim 14**. Fujii discloses a method wherein the determining of the likely location or locations includes: determining a set of likelihood components for each of a set of locations, each component corresponding to a respective managed access point whose transmissions are listened for at the particular station, and determining an overall likelihood for each of the set of locations as the product of the likelihood components (paragraph 46, read as a diagram indicating the locations at which regularly registered APs that can be connected to the network).

Consider **claim 16 and as applied to claim 1**. Fujii and Whelan discloses a method wherein further comprising combining the results of the analyzing step with the results of one or more complementary rogue AP detection techniques (paragraphs 46 and 47).

Consider **claim 17 and as applied to claim 16**. Fujii and Whelan discloses a method wherein one of the complementary rogue AP detection techniques includes a client reporting to a managed AP a failed previous authentication attempt with an AP (Whelan; paragraph 30, read as Unlike conventional access points that only report mobile units that successfully associate with the access point or fail to associate for various reasons such as for example not being a member of an Access Control List (ACL), the access point agent is configured to report or store for later retrieval all wireless devices heard by the access point).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated the teachings of Whelan into the method of Fujii in order to allow the authorized access points to continuously listen for wireless traffic and

therefore being able to determined whether or not an access point is a member of an Access

Control List (paragraph 30).

Consider **claim 19 and as applied to claim 18**. The combination of Fujii and Whelan

disclose a method wherein the scan request includes a request to scan for beacons and probe

responses on the respective serving channel of each respective wireless AP or client station and

to report the results of the listening.

Consider **claim 20 and as applied to claim 18**. Fujii discloses a method wherein the

scan request a includes a request for the listening stations AP or client station to temporarily

listen for beacons and probe responses on a channel specified in the request and to report the

results of the listening (paragraphs 37 and 38).

Consider **claim 21 and as applied to claim 18**. Fujii and Whelan disclose a method

wherein the scan request from the WLAN manager and the scan report to the WLAN manager

use a protocol that provides for and encapsulates scan request messages and scan report

messages in IP packets (Whelan; paragraph 26).

Consider **claim 22 and as applied to claim 21**. Fujii and Whelan disclose a method

wherein the request from an AP to a client station, and the report from the client station to an AP

uses MAC frames (Whelan; paragraphs 17 and 39).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to have incorporated the teachings of Whelan into the method of Fujii in

order to be able to easily implement a switch or router configured to transfer information

between at least two network segments; and the network monitor is further configured to

configure the switch or router to prevent transfer of information through the switch originating from or addressed to the unauthorized access point (paragraph 17).

Consider **claim 23 and as applied to claim 21**. The combination of Fujii and Whelan disclose a method wherein the scan request includes a set of scan parameters that describe how information is to be obtained about beacons and probe responses received by the managed AP or clients thereof.

Consider **claim 24 and as applied to claim 23**. Fujii discloses a method wherein the scan parameters include one or more of: whether the request scan is an active scan or a passive scan or both an active and passive scan, and if an active scan, one or more channels for the active scan, the schedule of how often scans are to be performed, and whether the performing of the scan is to be by the AP receiving the scan request, the managed clients thereof, or both the AP and AP's clients (paragraphs 37 and 38, read as electromagnetic waves are scanned in order to search for APs to which the client can be connected).

Consider **claim 25 and as applied to claim 23**. Fujii discloses a method wherein after receiving the task request, the receiving AP sets up tasking according to the scan request, including scheduling any scans to be performed by the receiving AP itself, and also, in the case the tasking includes scanning by one or more clients, scheduling scans to be performed by the clients by sending request frames to the appropriate clients (paragraphs, 41 and 42, read as during the scan and AP search process, the clients receive information on the channels of APs from which they can receive electromagnetic waves. Then, each of the clients obtains an AP list.

The standby time is used in order to receive AP lists, which are temporally randomly transmitted

by any of the plurality of clients).

Conclusion

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to:**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Christopher M. Brandt whose telephone number is (571) 270-

1098. The examiner can normally be reached on 7:30a.m. to 5p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nick Corsaro can be reached on (571) 272-7876. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

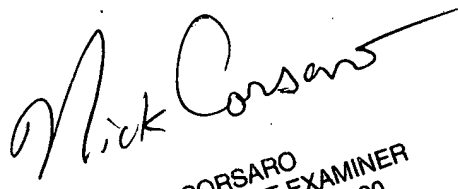information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist/customer service whose telephone number is (571) 272-

2600.

Christopher M. Brandt

C.M.B./cmb

December 18, 2006

NICK CORSARO
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600